Proceedings

2012

Network and Distributed System Security Symposium

Proceedings

2012

Network and Distributed System Security Symposium

February 5 - 8, 2012

San Diego, California

Sponsored by the

Internet Society

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108

Address your correspondence to: Senior Events Manager, Internet Society, 1775 Wiehle Avenue, Suite 201, Reston, Virginia 20190-5108, U.S.A., tel. +1 703 439 2120, fax +1 703 326 9881, orders@isoc.org.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.

ISBN Number (Digital Format) 1-891562-33-9

Additional copies may be ordered from:

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108
tel +1 703.439.2120
fax +1 703.326.9881
http://www.isoc.org/

Table of Contents

SESSION 1: Networking I

SESSION 2: Social Networks and User Behavior I

SESSION 3: Mobile Networks

You Can Run, but You Can't Hide: Exposing Network Location for Targeted DoS Attacks in Cellular Networks
Z. Qian, Z. Want, Q Xu, Z.M. Mao, M. Zhang, Y-M. Wang

Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication
N. Golde, K. Redon, R. Borgaonkar

SESSION 4: Clouds/Crypto

Privacy-Preserving Logarithmic-time Search on Encrypted Data in Cloud
Y. Luhh

Large-Scale Privacy-Preserving Mapping of Human Genomic Sequences on Hybrid Clouds
Y. Chen, B. Peng, X.F. Wang, H. Tang

Making Argument Systems for Outsourced Computation Practical (Sometimes)
S. Setty, R. McPherson, A.J. Blumberg, M. Walfish

Towards Practical Oblivious RAM
E. Stefanov, E. Shi, D. Song

SESSION 5: Invited Papers

Hubble: Transparent and Extensible Malware Analysis by Combining Hardware Virtualization and Software Emulation
L. Yan, M. Jayachandra, M. Zhang, H. Yin

FreeMarket: Shopping for Free in Android Applications
D. Reynaud, D. Song, T. Magrino, E. Wu, R. Shin

Distance Hijacking Attacks on Distance Bounding Protocols
C. Cremers, K.B. Rasmussen, S. Capkun

Throttling Tor Bandwidth Parasites
R. Jansen, N. Hopper, P. Syverson

Taking Routers Off Their Meds: Why Assumptions of Router Stability are Dangerous
M. Schuchard, C. Thompson, N. Hopper, Y. Kim

Newton Meets Vivaldi: Using Physical Laws to Secure Virtual Coordinate Systems
J. Seibert, S. Becker, C. Nita-Rotaru, R. State

Charm: A Framework for Rapidly Prototyping Cryptosystems
J.A. Akinyele, M.D. Green, A.D. Rubin

Abuse Detection and Prevention Systems at a Large Scale Video Sharing Website
Y-T. Chen, P. Grinspan, B. Linvingston, P. Nandy, B. Palmer

SESSION 6: Applied Crypto

Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation
M.S.Islam, M. Kuzu, M. Kantarcioglu

On Limitations of Designing Leakage-Resilient Password Systems: Attacks, Principles and Usability
Q. Yan, J. Han, Y. Li, R.H. Deng

Adaptive Password-Strength Meters from Markov Models
C. Castelluccia, M. Dürmuth, D. Perito

Private Set Intersection: Are Garbled Circuits Better than Custom Protocols?
Y. Huang, D. Evans, J. Katz

Keynote Speaker: Stephen E. Schmidt,
Chief Information Security Officer, Amazon Web Services

SESSION 7: Smartphones

Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications
S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, E. Weippl

MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones
L. Davi, A. Dmitrienko, M. Egele, T. Fischer, T. Holz, R. Hund, S. Nürnberger, A-R. Sadeghi

Towards Taming Privilege-Escalation Attacks on Android
S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, A-R. Sadeghi, B. Shastry

Systematic Detection of Capability Leaks in Stock Android Smartphones
M. Grace, Y. Zhou, Z. Wang, X. Jiang

Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets
Y. Zhou, Z. Wang, W. Zhou, X. Jiang

Keynote Speaker: David Brin
Scientist and award-winning science-fiction author

SESSION 8: Social Networks and User Behavior II

Insights into User Behavior in Dealing with Internet Attacks
K. Onarlioglu, U.O. Yilmaz, E. Kirda, D. Balzarotti

PathCutter: Severing the Self-Propagation Path of XSS JavaScript Worms in Social Web Networks
Y. Cao, V. Yegneswaran, P. Porras, Y. Chen

The Latent Community Model for Detecting Sybils in Social Networks
Z. Cai, C. Jermaine

SESSION 9: Privacy and Anonymity

BLACR: TTP-Free Blacklistable Anonymous Credentials with Reputation
M.H. Au, A. Kapadia, W. Susilo

Accountable Wiretapping - or - I Know They Can Hear You Now
A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, D. Wallach

Shadow: Running Tor in a Box for Accurate and Efficient Experimentation
R. Jansen, N. Hopper

SESSION 10: Host Security

DIMSUM: Discovering Semantic Data of Interest from Un-mappable Memory with Confidence
Z. Lin, J. Rhee, C. Wu, X. Zhang, D. Xu

SecureSwitch: BIOS-Assisted Isolation and Switch between Trusted and Untrusted Commodity OSes
K. Sun, J. Wang, F. Zhang, A. Stavrou

SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust
K.E. Defrawy, A. Francillon, D. Perito, G. Tsudik

Kruiser: Semi-synchronized Non-blocking Concurrent Kernel Heap Buffer Overflow Monitoring
D. Tian, Q. Zeng, D. Wu, P. Liu, C. Hu

Keynote Speaker: Eric Grosse

Vice President - Security Engineering at Google

SESSION 11: Web

WarningBird: Detecting Suspicious URLs in Twitter Stream
S. Lee, J. Kim

Using Replicated Execution for a More Secure and Reliable Web Browser
H. Xue, N. Dautenhahn, S.T. King

Host Fingerprinting and Tracking on the Web: Privacy and Security Implications
T-F. Yen, Y. Xie, F. Yu, R.P. Yu, M. Abadi

SESSION 12: Networking II

SESSION 13: Distributed Systems

SESSION 14: Software

General Chair’s Message

It is my pleasure to welcome you to the Nineteenth Internet Society Symposium on Network and Distributed Systems Security, and to the Hilton Resort and Spa on Mission Bay. Those of you fortunate enough to have attended last year will notice some important changes.

The first and most obvious is that we are at the Hilton Resort and Spa for the first time in NDSS's history. All of you should be thanked for our growth and success that has allowed us to move to larger facilities. We believe you will find facilities and staff exceptional.

The second change you should notice is that we have added an additional half day to the symposium in order to cover all the exciting papers. This brings the meeting to three full days of material.

Every NDSS meeting introduces some changes. One feature that has remained consistent throughout the history of NDSS, however, is the superior quality of the technical program. Our research domain continues to emphasize practical applications of security based on solid theoretical foundations.The program stretches from canonical to current, and includes both the theoretical and the pressing need. This scope, along with a willingness to consider potentially controversial or unusual research, is the essential beauty of NDSS.

The program for this year includes fourteen sessions and 54 papers (almost double from last year) covering a variety of current security topics, including security in emerging applications, such as social networks, vehicular vulnerabilities and smart phones; wireless networks; operating system security; network malware; biometrics; program security and code analysis; web security; cloud computing; anonymity; cryptographic systems and privacy. We are also especially fortunate to have four fantastic keynote speakers this year: David Brin, scientist & award-winning science-fiction author; Eric Grosse, Vice President of Security Engineering at Google; Stephen E. Schmidt, Chief Information Security Officer, Amazon Web Services and John N. Stewart, Vice President & Chief Security Officer, Cisco Systems Inc.

Though the symposium revolves around the technical presentations, there is far more to the experience. The hall track, meeting new colleagues, asking questions, and participating in discussions are invaluable parts of the process of disseminating and discussing information. Take advantage of them. Remember also to take advantage at some point of the superior geographic location.

This symposium is possible only through the hard work of many people. The steering group, which I am pleased to co-chair with Lynn St. Amour from the Internet Society, expertly charts a course for the conference that keeps its focus current, relevant, and practical. Kevin Craemer has done a wonderful job of helping plan and publicize the conference. Andrew M. White skillfully assembled the Proceedings as Publications Chair with assistance from Terry Weigler. This meeting is as enjoyable and successful as it is because of the efforts of these people -- it is no exaggeration to say that NDSS simply would not happen without each of their contributions.

The quality of this conference directly depends upon the quality of the papers accepted. The program committee, under the direction of Program Chair Radu Sion has done a fantastic job and has selected an extraordinary set of papers. I thank Radu and the entire program committee for their expertise, hard work, and dedication. I also thank the authors who submitted papers and the speakers who are present; you are the core of this symposium.

I am also grateful for our sponsors as it would be impossible to hold such an event without you. Our sponsors are the Internet Society for overall sponsorship; Internet2 for Patron sponsorship; Afilias and the San Diego Supercomputer Center (SDSC) for Silver sponsorships; Microsoft Research and Google for Bronze sponsorships, and IEEE Security and Privacy Magazine as our media sponsor. The conference is organized by the Internet Society, in cooperation with USENIX.

This is my first year as General Chair of NDSS, moving up from my previous role as Local Arrangements Chair. I would also like to personally thank Ex-Chair Doug Szajda for his help and for mentoring me in my new role. I view it as a great honor to chair a conference where the attendees are some of the finest minds in computer security.

Thomas Hutton
San Diego Supercomputer Center
University of California, San Diego
hutton@sdsc.edu

Program Chair's Message

Dear Reader,

I am happy to present to you these proceedings of the 2012 Network and Distributed System Security Symposium (NDSS), held on 5-8 February, 2012, at the Hilton Resort & Spa in San Diego, California.

The symposium is organized by the Internet Society (ISOC) and this is its 19th instance. Since its inception in 1993, NDSS has been a premier forum on the latest developments in computer and network security research, bringing together both researchers and practitioners.

This year, we are pleased to have received *317 submissions*. After sanity checks and additional cleanup, a total of 258 excellent papers entered the *double-blind* reviewing process. A program committee meeting was co-hosted with the ACM CCS conference in Chicago. The PC had the difficult task of creating a program out of the large number of excellent submissions and accepted *46 research papers*. Since a large number of excellent papers didn't make it in, I took upon myself the task of inviting *all* remaining highly-ranked submissions for a special invited short-talks session. 8 papers accepted my invitation. Overall, the following per country distributions apply:

	Submitted papers	**Authors**	**Accepted Papers**	**Acceptance rate per country**
1	USA (141)	USA (424)	USA (30)	Luxembourg, Turkey (100%)
2	Germany (17)	Germany (45)	Germany (4)	Austria (75%)
3	China (10)	China (40)	Switzerland (2)	UK (50%)
4	Switzerland (8)	Canada (17)	France (2)	S. Korea (40%)
5	Singapore (7)	France (15)		France (28%)

The accepted papers cover diverse topic areas: Mobile, Cellular, Wired and Social Network Security, Smart-Phone Security, Cloud Computing Security, Applied Cryptography, Anonymity, Privacy, Host-Level Security, Software Analysis and many others.

In addition to the research program, the symposium features no less than four invited speakers:

- David Brin, PhD, American scientist and award-winning, New York Times best-selling author
- Eric Grosse, Vice President - Security Engineering at Google
- Stephen E. Schmidt, Chief Information Security Officer, Amazon Web Services, Amazon Inc.
- John N. Stewart, Vice President and Chief Security Officer, Cisco Systems Inc.

I would like to thank you, the reader and participant, the organizing committee, the hard-working program committee, the steering group, the ISOC staff, our sponsors, and most importantly, the authors of all the papers submitted to the symposium. I hope you will enjoy the program!

Radu Sion
Stony Brook Network Security and Applied Cryptography Lab
digitalpiglet@acm.org

Program Committee Members

Radu Sion, Stony Brook University (Chair)
Ross Anderson, University of Cambridge
Davide Balzarotti, EURECOM Sophia Antipolis
Lujo Bauer, Carnegie Mellon
Kosta Beznosov, University of British Columbia
Matt Bishop, UC Davis
Nikita Borisov, UIUC
Elie Bursztein, Stanford University
Christian Cachin, IBM Research Zurich
Bogdan Carbunar, Motorola Labs
Jeff Chase, Duke University
Yan Chen, Northwestern University
Landon Cox, Duke University
Marc Dacier, Symantec Research Labs
George Danezis, Microsoft Research
Sven Dietrich, Stevens Institute of Technology
Dave Evans, University of Virginia
Nick Feamster, Georgia Tech
Carrie Gates, CA Technologies
Russ Housley, Internet Engineering Task Force
Xuxian Jiang, North Carolina State University
Rob Johnson, Stony Brook University
Ari Juels, RSA Labs
Stefan Katzenbeisser, TU Darmstadt
Angelos Keromytis, Columbia University
Yongdae Kim, University of Minnesota
Wenke Lee, Georgia Tech
Brian Levine, UMASS Amherst
Morley Mao, University of Michigan
Patrick McDaniel, Penn State University
John Mitchell, Stanford University
David Molnar, Microsoft Research
Peng Ning, North Carolina State University
Cristina Nita-Rotaru, Purdue University
Bryan Parno, Microsoft Research
Vern Paxson, UC Berkeley / ICSI
Giuseppe Persiano, Universita di Salerno
Michael Reiter, UNC at Chapel Hill
Volker Roth, Freie Universitaet Berlin
Ahmad-Reza Sadeghi, Technical University Darmstadt
Nitesh Saxena, NYU Poly
R. Sekar, Stony Brook University
Elaine Shi, UC Berkeley and Parc
Vitaly Shmatikov, University of Texas at Austin
Alex Snoeren, UC San Diego
Robin Sommer, ICSI
Paul Syverson, Naval Research Laboratory
Doug Szajda, University of Richmond
Wade Trappe, Rutgers University
Arun Venkataramani, UMASS Amherst
Dan Wallach, Rice University
Cliff Wang, US Army Research Office
Helen Wang, Microsoft Research
Nick Weaver, ICSI
Peter Williams, Stony Brook University
Dongyan Xu, Purdue University
Moti Yung, Google Inc.

Conference Committee

General Chair
Thomas Hutton
San Diego Supercomputer Center @ UCSD
hutton@ucsd.edu

Program Chair
Radu Sion
Stony Brook Network Security and Applied Cryptography Lab
sion@cs.stonybrook.edu

Publications Chair
Andrew White
University of North Carolina
amw@cs.unc.edu

Publicity Chair
Kevin Craemer
Internet Society
craemer@isoc.org

Conference Coordinator
Kevin Craemer
Internet Society
craemer@isoc.org

Sponsorship Coordinator
Kevin Craemer
Internet Society
craemer@isoc.org

NDSS Steering Group

Co-Chairs

Thomas Hutton
San Diego Supercomputer Center
University of California, San Diego

Lynn St.Amour
Internet Society

Administrative Coordinator

Kevin Craemer
Internet Society

Steering Group Members

Lujo Bauer
Carnegie Mellon University

Tadayoshi (Yoshi) Kohno
University of Washington

Barry Lawson
University of Richmond

Wenke Lee
Georgia Institute of Technology

Clifford Neuman
University of Southern California

Adrian Perrig
Carnegie Mellon University

Michael Roe
University of Hertfordshire

Radu Sion
Stony Brook University

Doug Szajda
University of Richmond

Giovanni Vigna
University of California, Santa Barbara